

技術情報管理認証制度

## 監査の指針

---

## 目次

|                              |           |
|------------------------------|-----------|
| <b>1. 前文 .....</b>           | <b>3</b>  |
| <b>2. 監査の原則 .....</b>        | <b>4</b>  |
| <b>3. 監査の独立性について .....</b>   | <b>5</b>  |
| 3.1 独立性 .....                | 5         |
| 3.2 精神上的の独立性 .....           | 5         |
| 3.3 外観上の独立性 .....            | 5         |
| 3.3.1 内部部門による監査における独立性 ..... | 5         |
| 3.3.2 外部者による監査における独立性 .....  | 6         |
| <b>4. 監査の実施について .....</b>    | <b>8</b>  |
| 4.1 監査証拠の入手と評価 .....         | 8         |
| 4.2 監査調書の作成と保存 .....         | 8         |
| <b>5. 監査の報告について .....</b>    | <b>9</b>  |
| 5.1 監査報告書の提出と開示 .....        | 9         |
| 5.2 監査報告書の記載事項 .....         | 9         |
| 5.3 監査報告書のレビュー .....         | 9         |
| <b>付録：監査計画書ひな形 .....</b>     | <b>10</b> |
| <b>付録：監査報告書ひな形 .....</b>     | <b>11</b> |
| <b>付録：監査記録（例） .....</b>      | <b>12</b> |

## 1. 前文

本指針は、技術情報管理認証制度における事業者の内部監査で活用することを想定したものである。

技術情報管理認証制度における監査の目的は、技術等情報に関する管理が効果的に実施されるように、事業者が選択した基準において、適切な管理策の実施状況を、監査人が独立かつ専門的な立場から評価することにある。

技術情報管理は事業者の責任において行われるべきものであり、監査は事業者の技術等情報管理が有効に行われることを支援するものである。

技術情報管理認証制度における監査は、「情報セキュリティ監査基準」を元に実施することが求められるが、本指針は、特に監査において、監査人が遵守すべき事項等について示す。

なお、技術情報管理認証制度で作成する「監査ガイドライン」は、一義的には認証機関が審査を行う際に参照されるものであるが、監査においても活用可能である。

## 2. 監査の原則

監査において、適切かつ十分な結論を導き出すため、以下の原則を順守することが必要である。

### (1) 高潔さ

監査人は、監査業務を倫理的に、正直に、かつ責任感を持って行うことが望ましい。また、全ての対応について公正さを持ち、偏りなく行われることが望ましい。

### (2) 公正な報告

監査に関する報告は、ありのままに、かつ、正確に監査活動を反映することが望ましい。

### (3) 専門家としての正当な注意

監査人は、監査業務の重要性、及び監査業務に関わる利害関係者が監査を行う者に対して抱いている信頼に見合う正当な注意を払うことが望ましい。監査において根拠ある判断を行う能力を持つことが重要である。

### (4) 機密保持

監査人は、その任務において得た情報の利用及び保護について慎重であることが望ましい。

### (5) 独立性

監査人は、可能な限り監査の対象となる活動から独立した立場にあり、全ての場合において偏り及び利害抵触がない形で行動することが望ましい。小規模の組織においては、内部監査を行う者が完全に独立していることは可能でない場合もあるが、偏りをなくし、客観性を保つあらゆる努力を行うことが望ましい。

### (6) 証拠に基づくアプローチ

監査証拠は、検証可能なものであることが望ましい。監査証拠は、入手可能な情報からのサンプルに基づくことが望ましい。

### 3. 監査の独立性について

#### 3.1 独立性

技術情報管理認証制度では、「情報セキュリティ監査基準」と同様、監査を客観的に実施するために、監査人に対して監査対象から独立していることを求める。監査を客観的に実施することの要件として、精神上的の独立性だけでなく、外観上の独立性も監査人に求める。

#### 3.2 精神上的の独立性

監査人は、監査の実施にあたり、監査の専門家としての判断をゆがめるおそれのある諸要因から影響を受けない精神状態、及び客観性を確保し、専門家としての公正不偏な態度を堅持できる状態を保持していなければならない。

#### 3.3 外観上の独立性

監査人は、監査を客観的に実施するために、監査対象から独立していなければならない。認証取得を目的とした監査の場合、被監査主体と身分上、密接な利害関係を有することがあってはならない。

「情報セキュリティ監査人の独立性のガイドライン」によると、外観上の独立性とは、第三者から見た際に、誠実性、客観性が阻害されていると推測される次のような事実や環境を避けることである。

- 1) 禁止すべき利害関係（経済的利害関係）
- 2) 避けるべき外観（不適正な外観）

##### 3.3.1 内部部門による監査における独立性

技術情報管理認証制度における監査について、特定部門を被監査主体として内部部門が監査を実施する場合を想定すると、以下のような阻害要因を避ける必要がある。

内部部門による監査における外観上の独立性の阻害要因

| 阻害要因                  | 阻害要件の事例                                                                                                                                                                                                                                                                                                        |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1) 禁止すべき利害関係（経済的利害関係） | <ul style="list-style-type: none"><li>● 内部監査部門または内部監査人は、被監査主体と協力したビジネス活動に関与している</li><li>● 内部監査部門または内部監査人は、被監査主体の監査対象となる情報セキュリティの設計、構築、検査の業務に関わっている</li><li>● 内部監査部門または、被監査主体から便益や贈与を受けている</li><li>● 内部監査人は、自分自身に利害関係があり、または公正な判断に影響を及ぼすと合理的に推測される</li><li>● その他、内部監査部門に内部監査活動の目的および計画の達成を妨げるような制約がある</li></ul> |
| 2) 避けるべき外観（不適正な       | <ul style="list-style-type: none"><li>● 内部監査部門または内部監査人は、被監査主体の配下の部署に所属しておらず、組織上独立していない</li></ul>                                                                                                                                                                                                               |

|     |                                                                                                                                                                   |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 外観) | <ul style="list-style-type: none"> <li>● 必要な情報及び資料の入手が困難である</li> <li>● 内部監査部門または内部監査人は、助言勧告等がしにくい環境がある</li> <li>● 監査人が前事業年度に在籍していた組織（部門や子会社等）が被監査主体である</li> </ul> |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|

資料) 「情報セキュリティ監査人の独立性のガイドライン」  
(特定非営利活動法人 日本セキュリティ監査協会 審査委員会、2011 年)

具体的には、以下のような方法で独立性を確保することが考えられる。

＜独立性を確保する体制（例）＞

- 事業者の内部監査部門が情報管理に関わる監査を実施する。
- 本制度における被監査部門とは独立した内部監査部門または内部監査人を経営者が設置または任命する。
- 内部監査部門に専門知識が不足する場合は、情報管理や I T の専門知識を持ち、可能な限り客観的な立場である者を臨時監査人として経営者が任命し、監査部門を構成する。

### 3.3.2 外部者による監査における独立性

技術情報管理認証制度における監査について、事業者全体あるいは一部の部門を被監査主体として外部の者が監査を実施する場合を想定すると、以下のような阻害要因を避ける必要がある。

外部者による監査における外観上の独立性の阻害要因

| 阻害要因                  | 阻害要件の事例                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1) 禁止すべき利害関係（経済的利害関係） | <ul style="list-style-type: none"> <li>● 外部監査組織または監査人が、被監査主体から社会慣行を超える接待もしくは贈答を受けること、または、被監査主体に対して社会慣行を超える接待もしくは贈答を行う</li> <li>● 監査人及びその監査人の配偶者が、過去に被監査主体の役員、経営の意思決定に重要なかわりをもつ使用人等であった</li> <li>● 監査人と生計を一にする 2 親等以内の親族等が、被監査主体の株式を保有している</li> <li>● 外部監査組織及び監査人が提供する設計、構築または検査の業務に従事して、当該業務の結果を監査対象とする</li> <li>● 外部監査組織または監査人が被監査主体の経営者の意思決定に関与している</li> </ul> |
| 2) 避けるべき外観（不適正な外観）    | <ul style="list-style-type: none"> <li>● 特定の被監査主体または被監査主体のグループ企業から継続的に受け取る報酬が、監査人の収入の大部分を占める</li> <li>● 被監査主体のグループ企業が監査主体となり、グループ内の別の企業を被監査主体として監査を行う</li> </ul>                                                                                                                                                                                                 |

|  |                                                                                                                                                  |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>● 情報セキュリティ監査の言明書を監査人自らが作成したと受け取られる行為をする</li> <li>● 特定の被監査主体と監査人との間に訴訟が起きていることまたは起きる可能性が高い関係にある</li> </ul> |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------|

資料) 「情報セキュリティ監査人の独立性のガイドライン」  
(特定非営利活動法人 日本セキュリティ監査協会 審査委員会、2011 年)

## 4. 監査の実施について

### 4.1 監査証拠の入手と評価

監査人は、監査計画に基づいて、適切かつ慎重に監査手続を実施し、監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。

### 4.2 監査調書の作成と保存

監査人は、実施した監査手続の結果とその関連資料を、監査調書として作成しなければならない。監査調書は、監査結果の裏付けとなるため、監査の結論に至った過程がわかるように秩序整然と記録し、適切な方法によって保存しなければならない。



## 5. 監査の報告について

### 5.1 監査報告書の提出と開示

監査人は、実施した監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。監査報告書の外部への開示が必要とされる場合には、監査人は、監査の依頼者と慎重に協議の上で開示方法等を考慮しなければならない。

### 5.2 監査報告書の記載事項

監査報告書には、実施した監査の対象、実施した監査の概要について、監査人が必要と判断した事項を明瞭に記載しなければならない。

### 5.3 監査報告書のレビュー

監査報告書は、独立した立場の者によるレビューを受けること、もしくはピアレビュー（立場や職種の近い者が相互に評価・検証する形のレビュー）を行うこと等により、監査品質を確保することが望ましい。

付録：監査計画書ひな形

技術情報管理認証制度 監査計画書

日 付

1. 監査の目的

〇〇の情報に関する技術情報管理認証取得に向けた内部監査のため

2. 監査対象・日程等

| 事業所・部門 | 日程 | 監査人<br>(所属・氏名) | 備考 |
|--------|----|----------------|----|
|        |    |                |    |
|        |    |                |    |
|        |    |                |    |

3. 監査項目

| 監査項目 | 備考 |
|------|----|
|      |    |
|      |    |
|      |    |

## 付録：監査報告書ひな形

### 技術情報管理認証制度 監査報告書

日 付

宛 名

監査人署名

われわれは、公認情報セキュリティ主任監査人 氏名、情報セキュリティ監査人補 氏名からなる監査チームを組織し、「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準」に照らして、20xx 年 x 月 x 日から 20xx 年 x 月 x 日までの期間に係る XXX を対象として技術情報管理の状況について監査を実施した。われわれの責任は、監査手続を実施した結果に基づいて意見を表明することにある。

われわれの監査は、「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準」に準拠して行われた。監査は、技術情報の管理が効果的に実施されるよう、適切な管理策が採用されているか否かについて検討し評価している。採用した監査手続は、われわれが必要と認めたものを適用しており、監査の結果として意見表明のための合理的な根拠を得たと確信している。

われわれの意見によれば、20xx 年 x 月 x 日から 20xx 年 x 月 x 日までの期間に係る XXX を対象とした技術情報管理の実施状況は、「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準」に照らして適切であると認める。

付録：監査記録（例）

| 章 | 節  | 項 | 番   |                        | 内容                                                                                                                                                                       |                                                                                                                                      |                                                                                                                                            | 確認内容                                                                                |
|---|----|---|-----|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| I | 第四 | 1 | (1) | 共通事項                   | 管理対象情報の管理等                                                                                                                                                               | 管理対象情報の管理簿の作成等                                                                                                                       | 管理者は、持ち出し、複製、廃棄等の管理対象情報の状況を管理するための管理簿を作成する。                                                                                                | 管理対象情報管理簿(XX年XX月XX日～XX月XX日記録)を閲覧し、管理対象情報の持ち出し、複製、廃棄等の記録が示されていることを確認した。              |
|   |    | 6 | (1) |                        |                                                                                                                                                                          | 管理対象情報の適切な管理についての文書の作成等                                                                                                              | 事業者は、1から5までに定める手順のほか、第二の2により必要と決定した措置を実施するため、管理対象情報の適切な管理についての具体的な実現手法を記載した文書(以下「マニュアル」という。)を作成する。                                         | 管理対象情報の管理手法を示したマニュアル(XX年XX月XX日策定、第2版)を閲覧し、管理対象情報の適切な管理についての具体的な実現手法が記載されていることを確認した。 |
|   |    |   | (2) |                        |                                                                                                                                                                          | 事業者の取締役等の経営層(管理対象情報を活用し、事業を実施する部門の長を含む。)は、マニュアルを、当該管理対象情報を取り扱う可能性のある全ての者に周知する。                                                       | 管理対象情報の管理手法を示したマニュアルの周知記録(XX年度)を閲覧し、経営層がマニュアルを、管理対象情報を取り扱う可能性のある全ての者に周知していることを確認した。<br>管理対象情報を取り扱う製造部門の従業員へのインタビューにより、マニュアルを認識していることを確認した。 |                                                                                     |
|   | 第六 | 1 |     | 管理対象情報の漏えいの事故等の発生時等の報告 | 事業者は、アクセス権者を含む全ての従業員等に対して、管理対象情報へのアクセス権を有さない者がアクセス権者の近傍にいない状態で管理対象情報を取り扱っていることを発見した場合等当該管理対象情報の漏えいが発生し、又はその疑いがあると従業員等が認める場合に、直ちに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。 | 管理対象情報の漏えい事故を発見、または疑いがあると認めた場合、報告先として定められた技術等情報管理責任者に対して、報告をするように指示された文書(XX年XX月XX日)を確認した。<br>本文書が、翌週の各部門の朝礼で周知されたことを各部門からの週次報告で確認した。 |                                                                                                                                            |                                                                                     |